

Sylow p -groups of polynomial permutations on the integers mod p^n

Sophie Frisch and Daniel Krenn

Abstract. We enumerate and describe the Sylow p -groups of the group of polynomial permutations of the integers mod p^n . MSC 2000: primary 20D20, secondary 11T06, 13M10, 11C08, 13F20, 20E18.

1. Introduction

Fix a prime p and let $n \in \mathbb{N}$. Every polynomial $f \in \mathbb{Z}[x]$ defines a function from $\mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$ to itself. If this function happens to be bijective, it is called a *polynomial permutation* of \mathbb{Z}_{p^n} . The polynomial permutations of \mathbb{Z}_{p^n} form a group (G_n, \circ) with respect to composition. The order of this group has been known since at least 1921 (Kempner [10]) to be

$$|G_2| = p!(p-1)^p p^p \quad \text{and} \quad |G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^n \beta(k)} \quad \text{for } n \geq 3,$$

where $\beta(k)$ is the least n such that p^k divides $n!$, but the structure of (G_n, \circ) is elusive. (See, however, Nöbauer [15] for some partial results). Since the order of G_n is divisible by a high power of $(p-1)$ for large p , even the number of Sylow p -groups is not obvious.

We will show that there are $(p-1)!(p-1)^{p-2}$ Sylow p -groups of G_n and describe these Sylow p -groups, see Theorem 4.5.

Some notation: p is a fixed prime throughout. A function $g: \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$ arising from a polynomial in $\mathbb{Z}_{p^n}[x]$ or, equivalently, from a polynomial in $\mathbb{Z}[x]$, is called a *polynomial function* on \mathbb{Z}_{p^n} . We denote by (F_n, \circ) the monoid with respect to composition of polynomial functions on \mathbb{Z}_{p^n} , and by (G_n, \circ) its group of units, the group of polynomial permutations of \mathbb{Z}_{p^n} .

The natural projection of polynomial functions on $\mathbb{Z}_{p^{n+1}}$ onto polynomial functions on \mathbb{Z}_{p^n} we write as $\pi_n: F_{n+1} \rightarrow F_n$. If f is a polynomial in $\mathbb{Z}[x]$

Sophie Frisch is supported by the Austrian Science Fund (FWF), grant P23245-N18.

Daniel Krenn is supported by the Austrian Science Fund (FWF), project W1230 doctoral program “Discrete Mathematics”.

(or in $\mathbb{Z}_{p^m}[x]$ for $m \geq n$) we denote the polynomial function on $\mathbb{Z}_{p^n}[x]$ induced by f by $[f]_{p^n}$.

The order of F_n and that of G_n have been determined by Kempner [10] in a rather complicated manner. His results were cast into a simpler form by Nöbauer [14] and Keller and Olson [9] among others. Since then there have been many generalizations of the order formulas to more general finite rings [16, 13, 2, 6, 1, 8, 7]. Also, polynomial permutations in several variables (permutations of $(\mathbb{Z}_{p^n})^k$ defined by k -tuples of polynomials in k variables) have been looked into [5, 4, 19, 17, 18, 11].

2. Polynomial functions and permutations

To put things in context, we recall some well-known facts, to be found, among other places, in [10, 14, 3, 9]. The reader familiar with polynomial functions on finite rings is encouraged to skip to section 3. (Reviewers take note that we do not claim anything in section 2 as new!)

Definition. For p prime and $n \in \mathbb{N}$, let

$$\alpha_p(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \quad \text{and} \quad \beta_p(n) = \min\{m \mid \alpha_p(m) \geq n\}.$$

If p is fixed, we just write $\alpha(n)$ and $\beta(n)$.

Notation. For $k \in \mathbb{N}$, let $(x)_k = x(x-1)\dots(x-k+1)$ and $(x)_0 = 1$. We denote p -adic valuation by v_p .

2.1 Fact.

- (1) $\alpha_p(n) = v_p(n!)$.
- (2) For $1 \leq k \leq p$, $\beta_p(k) = kp$ and for $k > p$, $\beta_p(k) < kp$.
- (3) For all $n \in \mathbb{Z}$, $v_p((n)_k) \geq \alpha_p(k)$; and $v_p((k)_k) = v_p(k!) = \alpha_p(k)$.

Proof. Easy. \square

Remark. The sequence $(\beta_p(n))_{n=1}^{\infty}$ is obtained by going through the natural numbers in increasing order and repeating each $k \in \mathbb{N}$ $v_p(k)$ times. For instance, $\beta_2(n)$ for $n \geq 1$ is: 2, 4, 4, 6, 8, 8, 8, 10, 12, 12, 14, 16, 16, 16, 16, 18, 20, 20, ...

The falling factorials $(x)_0 = 1$, $(x)_k = x(x-1)\dots(x-k+1)$, $k > 0$, form a basis of the free \mathbb{Z} -module $\mathbb{Z}[x]$, and representation with respect to this basis gives a convenient canonical form for a polynomial representing a given polynomial function on \mathbb{Z}_{p^n} .

2.2 Fact. A polynomial $f \in \mathbb{Z}[x]$, $f = \sum_k a_k (x)_k$, induces the zero-function mod p^n if and only if $a_k \equiv 0 \pmod{p^{n-\alpha(k)}}$ for all k (or, equivalently, for all $k < \beta(n)$).

Proof. Induction on k using the facts that $(m)_k = 0$ for $m < k$, that $v_p((n)_k) \geq \alpha_p(k)$ for all $n \in \mathbb{Z}$, and that $v_p((k)_k) = v_p(k!) = \alpha_p(k)$. \square

2.3 Corollary. Every polynomial function on \mathbb{Z}_{p^n} is represented by a unique $f \in \mathbb{Z}[x]$ of the form $f = \sum_{k=0}^{\beta(n)-1} a_k (x)_k$, with $0 \leq a_k < p^{n-\alpha(k)}$ for all k .

Comparing the canonical forms of polynomial functions mod p^n with those mod p^{n-1} we see that every polynomial function mod p^{n-1} gives rise to $p^{\beta(n)}$ different polynomial functions mod p^n :

2.4 Corollary. Let (F_n, \circ) be the monoid of polynomial functions on \mathbb{Z}_{p^n} with respect to composition and $\pi_n : F_{n+1} \rightarrow F_n$ the canonical projection.

- (1) For all $n \geq 1$ and for each $f \in F_n$ we have $|\pi_n^{-1}(f)| = p^{\beta(n+1)}$.
- (2) For all $n \geq 1$, the number of polynomial functions on \mathbb{Z}_{p^n} is

$$|F_n| = p^{\sum_{k=1}^n \beta(k)}.$$

Notation. We write $[f]_{p^n}$ for the function defined by $f \in \mathbb{Z}[x]$ on \mathbb{Z}_{p^n} .

2.5 Lemma. Every polynomial $f \in \mathbb{Z}[x]$ is uniquely representable as

$$f(x) = f_0(x) + f_1(x)(x^p - x) + f_2(x)(x^p - x)^2 + \dots + f_m(x)(x^p - x)^m + \dots$$

with $f_m \in \mathbb{Z}[x]$, $\deg f_m < p$, for all $m \geq 0$. Now let $f, g \in \mathbb{Z}[x]$.

- (1) If $n \leq p$, then $[f]_{p^n} = [g]_{p^n}$ is equivalent to: $f_k = g_k \pmod{p^{n-k}\mathbb{Z}[x]}$ for $0 \leq k < n$.
- (2) $[f]_{p^2} = [g]_{p^2}$ is equivalent to: $f_0 = g_0 \pmod{p^2\mathbb{Z}[x]}$ and $f_1 = g_1 \pmod{p\mathbb{Z}[x]}$.
- (3) $[f]_p = [g]_p$ and $[f']_p = [g']_p$ is equivalent to: $f_0 = g_0 \pmod{p\mathbb{Z}[x]}$ and $f_1 = g_1 \pmod{p\mathbb{Z}[x]}$.

Proof. The canonical representation is obtained by repeated division with remainder by $(x^p - x)$, and uniqueness follows from uniqueness of quotient and remainder of polynomial division. Note that $[f]_p = [f_0]_p$ and $[f']_p = [f'_0 - f_1]_p$. This gives (3).

Denote by $f \sim g$ the equivalence relation $f_k = g_k \pmod{p^{n-k}\mathbb{Z}[x]}$ for $0 \leq k < n$. Then $f \sim g$ implies $[f]_{p^n} = [g]_{p^n}$. There are $p^{p+2p+3p+\dots+np}$ equivalence classes of \sim and $p^{\beta(1)+\beta(2)+\beta(3)+\dots+\beta(n)}$ different $[f]_{p^n}$. For $k \leq p$, $\beta(k) = kp$. Therefore the equivalence relations $f \sim g$ and $[f]_{p^n} = [g]_{p^n}$ coincide. This gives (1), and (2) is just the special case $n = 2$. \square

We can rephrase this in terms of ideals of $\mathbb{Z}[x]$.

2.6 Corollary. *For every $n \in \mathbb{N}$, consider the two ideals of $\mathbb{Z}[x]$*

$$I_n = \{f \in \mathbb{Z}[x] \mid f(\mathbb{Z}) \subseteq p^n \mathbb{Z}\} \quad \text{and} \quad J_n = (\{p^{n-k}(x^p - x)^k \mid 0 \leq k \leq n\}).$$

Then $[\mathbb{Z}[x] : I_n] = p^{\beta(1)+\beta(2)+\beta(3)+\dots+\beta(n)}$ and $[\mathbb{Z}[x] : J_n] = p^{p+2p+3p+\dots+np}$. Therefore, $J_n = I_n$ for $n \leq p$, whereas for $n > p$, J_n is properly contained in I_n .

Proof. $J_n \subseteq I_n$. The index of J_n in $\mathbb{Z}[x]$ is $p^{p+2p+3p+\dots+np}$, because $f \in J_n$ if and only if $f_k = 0 \pmod{p^{n-k}\mathbb{Z}[x]}$ for $0 \leq k < n$ in the canonical representation of Lemma 2.5. The index of I_n in $\mathbb{Z}[x]$ is $p^{\beta(1)+\beta(2)+\beta(3)+\dots+\beta(n)}$ by Corollary 2.4 (2) and $[\mathbb{Z}[x] : I_n] < [\mathbb{Z}[x] : J_n]$ if and only if $n > p$ by Fact 2.1 (2). \square

2.7 Fact. (cf. McDonald [12]) *Let $n \geq 2$. The function on \mathbb{Z}_{p^n} induced by a polynomial $f \in \mathbb{Z}[x]$ is a permutation if and only if*

- (1) *f induces a permutation of \mathbb{Z}_p and*
- (2) *the derivative f' has no zero mod p .*

2.8 Lemma. *Let $[f]_{p^n}$ and $[f]_p$ be the functions defined by $f \in \mathbb{Z}[x]$ on \mathbb{Z}_{p^n} and \mathbb{Z}_p , respectively, and $[f']_p$ the function defined by the formal derivative of f on \mathbb{Z}_p . Then*

- (1) *$[f]_{p^2}$ determines not just $[f]_p$, but also $[f']_p$.*
- (2) *Let $n \geq 2$. Then $[f]_{p^n}$ is a permutation if and only if $[f]_{p^2}$ is a permutation.*
- (3) *For every pair of functions (α, β) , $\alpha : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $\beta : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, there are exactly p^p polynomial functions $[f]_{p^2}$ on \mathbb{Z}_{p^2} with $[f]_p = \alpha$ and $[f']_p = \beta$.*
- (4) *For every pair of functions (α, β) , $\alpha : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ bijective, $\beta : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \setminus \{0\}$, there are exactly p^p polynomial permutations $[f]_{p^2}$ on \mathbb{Z}_{p^2} with $[f]_p = \alpha$ and $[f']_p = \beta$.*

Proof. (1) and (3) follow immediately from Lemma 2.5 for $n = 2$ and (2) and (4) then follow from Fact 2.7. \square

2.9 Remark. Lemma 2.8 (2) implies that the inverse image of G_n under $\pi_n : F_{n+1} \rightarrow F_n$ is G_{n+1} . We denote by $\pi_n : G_{n+1} \rightarrow G_n$ the restriction of π_n to G_n . Then Corollary 2.4 implies, for all $n \geq 2$,

$$|\ker(\pi_n)| = p^{\beta(n+1)}.$$

2.10 Corollary. *The number of polynomial permutations on \mathbb{Z}_{p^2} is*

$$|G_2| = p!(p-1)^p p^p$$

and for $n \geq 3$ the number of polynomial permutations on \mathbb{Z}_{p^2} is

$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^n \beta(k)}.$$

Proof. In the canonical representation of $f \in \mathbb{Z}[x]$ in Lemma 2.5, there are $p!(p-1)^p$ choices of coefficients mod p for f_0 and f_1 such that the criteria of Fact 2.7 for a polynomial permutation on \mathbb{Z}_{p^2} are satisfied. And for each such choice there are p^p possibilities for the coefficients of f_0 mod p^2 . The coefficients of f_0 mod p^2 and those of f_1 mod p then determine the polynomial function mod p^2 . So $|G_2| = p!(p-1)^p p^p$. The formula for $|G_n|$ then follows from Remark 2.9. \square

This concludes our review of polynomial functions and polynomial permutations on \mathbb{Z}_{p^n} . We will now introduce a homomorphic image of G_2 whose Sylow p -groups bijectively correspond to the Sylow p -groups of G_n for any $n \geq 2$.

3. A group between G_1 and G_2

Into the projective system of monoids (F_n, \circ) we insert an extra semi-group E between F_1 and F_2 by means of monoid epimorphisms $\theta : F_2 \rightarrow E$ and $\psi : E \rightarrow F_1$ with $\psi\theta = \pi_1$.

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \dots$$

The restrictions of θ to G_2 and of ψ to the group of units H of E will be group-epimorphisms, so that we also insert an extra group H between G_2 and G_1 into the projective system of the G_i .

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \dots$$

In the following definition of E and H , f and f' are just two different names for functions. The connection with polynomials and their formal derivatives suggested by the notation will appear when we define θ and ψ .

Definition. We define the semi-group (E, \circ) by

$$E = \{(f, f') \mid f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p, f' : \mathbb{Z}_p \rightarrow \mathbb{Z}_p\}$$

with law of composition

$$(f, f') \circ (g, g') = (f \circ g, (f' \circ g) \cdot g'),$$

where $(f \circ g)(x) = f(g(x))$ and $((f' \circ g) \cdot g')(x) = f'(g(x)) \cdot g'(x)$.

We denote by (H, \circ) the group of units of E .

3.1 Lemma.

- (1) *The identity element of E is $(\iota, 1)$, with ι denoting the identity function on \mathbb{Z}_p and 1 the constant function 1.*
- (2) *The group of units of E has the form*

$$H = \{(f, f') \mid f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \text{ bijective, } f' : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \setminus \{0\}\}.$$

- (3) *The inverse of $(g, g') \in H$ is*

$$(g, g')^{-1} = (g^{-1}, \frac{1}{g' \circ g^{-1}}),$$

where g^{-1} is the inverse permutation of the permutation g and $1/a$ stands for the multiplicative inverse of a non-zero element $a \in \mathbb{Z}_p$, such that

$$(\frac{1}{g' \circ g^{-1}})(x) = \frac{1}{g'(g^{-1}(x))}$$

means the multiplicative inverse in $\mathbb{Z}_p \setminus \{0\}$ of $g'(g^{-1}(x))$.

Note that H is just a wreath product (designed to act on the left) of the permutation group S_p and a cyclic group of $p-1$ elements (here appearing as the multiplicative group of units of \mathbb{Z}_p).

Now for the homomorphisms θ and ψ .

Definition. We define $\psi : E \longrightarrow F_1$ by $\psi(f, f') = f$. As for $\theta : F_2 \rightarrow E$, given an element $[g]_{p^2} \in F_2$, set $\theta([g]_{p^2}) = ([g]_p, [g']_p)$ – this is well-defined by Lemma 2.8 (1).

3.2 Lemma.

- (i) $\theta : F_2 \rightarrow E$ is a monoid-epimorphism.
- (ii) The inverse image of H under $\theta : F_2 \rightarrow E$ is G_2 .
- (iii) The restriction of θ to G_2 is a group epimorphism $\theta : G_2 \rightarrow H$ with $|\ker(\theta)| = p^p$.
- (iv) $\psi : E \rightarrow F_1$ is a monoid epimorphism and ψ restricted to H is a group-epimorphism $\psi : H \rightarrow G_1$.

Proof. (i) follows from Lemma 2.8 (3) and (ii) from Fact 2.7. (iii) follows from Lemma 2.8 (4). Finally, (iv) holds because every function on \mathbb{Z}_p is a polynomial function and every permutation of \mathbb{Z}_p is a polynomial permutation. \square

4. Sylow subgroups of H and G_n

We will first determine the Sylow p -groups of H . The Sylow p -groups of G_n for $n \geq 2$ then are obtained as the inverse images of the Sylow p -groups of H under the epimorphism $G_n \rightarrow H$.

4.1 Lemma. *Let C_0 be the subgroup of S_p generated by the p -cycle $(0\ 1\ 2\ \dots\ p-1)$. Then one Sylow p -subgroup of H is*

$$S = \{(f, f') \in H \mid f \in C_0, f' = 1\},$$

where $f' = 1$ means the constant function 1. The normalizer of S in H is

$$N_H(S) = \{(g, g') \mid g \in N_{S_p}(C_0), g' \text{ a non-zero constant}\}.$$

Proof. As $|H| = p!(p-1)^p$, and S is a subgroup of H of order p , S is a Sylow p -group of H . Conjugation of $(f, f') \in S$ by $(g, g') \in H$ (using the fact that $f' = 1$) gives

$$(g, g')^{-1}(f, f')(g, g') = (g^{-1}, \frac{1}{g' \circ g^{-1}})(f \circ g, g') = (g^{-1} \circ f \circ g, \frac{g'}{g' \circ g^{-1} \circ f \circ g})$$

The first coordinate of $(g, g')^{-1}(f, f')(g, g')$ being in C_0 for all $(f, f') \in S$ is equivalent to $g \in N_{S_p}(C_0)$. The second coordinate of $(g, g')^{-1}(f, f')(g, g')$ being the constant function 1 for all $(f, f') \in S$ is equivalent to

$$\forall x \in \mathbb{Z}_p \quad g'(x) = g'(g^{-1}(f(g(x)))),$$

which is equivalent to g' being constant on every cycle of $g^{-1}fg$, which is equivalent to g' being constant on \mathbb{Z}_p , since f can be chosen to be a p -cycle. \square

4.2 Lemma. *Another way of describing the normalizer of S in H is*

$$N_H(S) = \{(f, f') \in H \mid \exists k \neq 0 \forall a, b \ f(a) - f(b) = k(a - b); \ f' \text{ a non-zero constant}\}.$$

Therefore, $|N_H(S)| = p(p-1)^2$ and $[H : N_H(S)] = (p-1)!(p-1)^{p-2}$.

Proof. Let $\sigma = (0\ 1\ 2 \dots p-1)$ and $f \in S_p$ then

$$f\sigma f^{-1} = (f(0)\ f(1)\ f(2) \dots f(p-1))$$

Now $f \in N_{S_p}(C_0)$ if and only if, for some $1 \leq k < p$ $f\sigma f^{-1} = \sigma^k$, i.e.,

$$(f(0)\ f(1)\ f(2) \dots f(p-1)) = (0\ k\ 2k \dots (p-1)k),$$

all numbers taken mod p . This is equivalent to $f(x+1) = f(x) + k$ or

$$f(x+1) - f(x) = k$$

and further equivalent to $f(a) - f(b) = k(a - b)$. Thus k and $f(0)$ determine $f \in N_{S_p}(C_0)$, and there are $(p-1)$ choices for k and p choices for $f(0)$. Together with the $(p-1)$ choices for the non-zero constant f' this makes $p(p-1)^2$ elements of $N_H(S)$. \square

4.3 Corollary. *There are $(p-1)!(p-1)^{p-2}$ Sylow p -subgroups of H .*

4.4 Theorem. *The Sylow p -subgroups of H are in bijective correspondence with pairs $(C, \bar{\varphi})$, where C is a cyclic subgroup of order p of S_p , $\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \setminus \{0\}$ is a function and $\bar{\varphi}$ is the class of φ with respect to the equivalence relation of multiplication by a non-zero constant. The subgroup corresponding to $(C, \bar{\varphi})$ is*

$$S_{(C, \bar{\varphi})} = \{(f, f') \in H \mid f \in C, \ f'(x) = \frac{\varphi(f(x))}{\varphi(x)}\}$$

Proof. Observe that each $S_{(C, \bar{\varphi})}$ is a subgroup of order p of H . Different pairs $(C, \bar{\varphi})$ give rise to different groups: Suppose $S_{(C, \bar{\varphi})} = S_{(D, \bar{\psi})}$. Then $C = D$ and for all $x \in \mathbb{Z}_p$ and for all $f \in C$ we get

$$\frac{\varphi(f(x))}{\varphi(x)} = \frac{\psi(f(x))}{\psi(x)}.$$

As C is transitive on \mathbb{Z}_p the latter condition is equivalent to

$$\forall x, y \in \mathbb{Z}_p \quad \frac{\psi(x)}{\varphi(x)} = \frac{\psi(y)}{\varphi(y)},$$

which means that $\varphi = k\psi$ for a nonzero $k \in \mathbb{Z}_p$.

There are $(p-2)!$ cyclic subgroups of order p of S_p , and $(p-1)^{p-1}$ equivalence classes $\bar{\varphi}$ of functions $\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \setminus \{0\}$. So the number of pairs $(C, \bar{\varphi})$ equals $(p-1)!(p-1)^{p-2}$, which is the number of Sylow p -groups of H , by the preceding corollary. \square

In the projective system of groups

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} \dots \xleftarrow{\pi_{n-1}} G_n$$

the kernel of the group epimorphism $G_n \rightarrow H$ is a finite p -group for every $n \geq 2$, because, firstly, the kernel of $\pi_{n-1} : G_n \rightarrow G_{n-1}$ is of order $p^{\beta(n)}$ by Remark 2.9, and secondly, the kernel of $\theta : G_2 \rightarrow H$ is of order p^p by Lemma 3.2 (iii). So the Sylow p -groups of G_n for $n \geq 2$ are just the inverse images of the Sylow p -groups of H :

4.5 Theorem. *Let $n \geq 2$. Let G_n be the group (with respect to composition) of polynomial permutations on \mathbb{Z}_{p^n} . There are $(p-1)!(p-1)^{p-2}$ Sylow p -groups of G_n . They are in bijective correspondence with pairs $(C, \bar{\varphi})$, where C is a cyclic subgroup of order p of S_p , $\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \setminus \{0\}$ a function and $\bar{\varphi}$ its class with respect to the equivalence relation of multiplication by a non-zero constant. The subgroup corresponding to $(C, \bar{\varphi})$ is*

$$S_{(C, \bar{\varphi})} = \{[f]_{p^n} \in G_n \mid [f]_p \in C, [f']_p(x) = \frac{\varphi([f]_p(x))}{\varphi(x)}\}.$$

One particularly easy to describe Sylow p -group of G_n corresponds to a constant function φ and the subgroup C generated by $(0 \ 1 \ 2 \dots p-1)$ of S_p . It is the inverse image of S defined in Lemma 4.1 and consists of those polynomial functions on \mathbb{Z}_{p^n} which are mod p a power of $(0 \ 1 \ 2 \dots p-1)$, and whose derivative is constant 1 mod p .

One last remark: Each Sylow p -group of $G_1 = S_p$ is isomorphic to C_p , where C_p denotes the cyclic group of order p . Also, it is not difficult to see (using the description of G_2 in [6]) that the Sylow p -groups of G_2 are of the form $C_p \wr C_p$. It is an open question, posed by W. Herfort (personal communication), if every finite wreath product $C_p \wr C_p \wr \dots \wr C_p$ of cyclic groups of order p can be embedded in G_n for some n .

References

- [1] M. BHARGAVA, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew. Math., 490 (1997), pp. 101–127.
- [2] J. V. BRAWLEY AND G. L. MULLEN, *Functions and polynomials over Galois rings*, J. Number Theory, 41 (1992), pp. 156–166.
- [3] L. CARLITZ, *Functions and polynomials (mod p^n)*, Acta Arith., 9 (1964), pp. 67–78.

- [4] Z. CHEN, *On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ to \mathbb{Z}_m* , Discrete Math., 162 (1996), pp. 67–76.
- [5] S. FRISCH, *When are weak permutation polynomials strong?*, Finite Fields Appl., 1 (1995), pp. 437–439.
- [6] ———, *Polynomial functions on finite commutative rings*, in Advances in commutative ring theory (Fez, 1997), vol. 205 of Lecture Notes in Pure and Appl. Math., Dekker, New York, 1999, pp. 323–336.
- [7] J. JIANG, *A note on polynomial functions over finite commutative rings*, Adv. Math. (China), 39 (2010), pp. 555–560.
- [8] J. J. JIANG, G. H. PENG, Q. SUN, AND Q. ZHANG, *On polynomial functions over finite commutative rings*, Acta Math. Sin. (Engl. Ser.), 22 (2006), pp. 1047–1050.
- [9] G. KELLER AND F. OLSON, *Counting polynomial functions (mod p^n)*, Duke Math. J., 35 (1968), pp. 835–838.
- [10] A. J. KEMPNER, *Polynomials and their residue systems*, Trans. Amer. Math. Soc., 22 (1921), pp. 240–266, 267–288.
- [11] N. P. LIU AND J. J. JIANG, *Polynomial functions in n variables over a finite commutative ring*, Sichuan Daxue Xuebao, 46 (2009), pp. 44–46.
- [12] B. R. McDONALD, *Finite Rings with Identity*, Dekker, 1974.
- [13] A. NECHAEV, *Polynomial transformations of finite commutative local rings of principal ideals*, Math. Notes, 27 (1980), pp. 425–432. transl. from Mat. Zametki 27 (1980) 885–897, 989.
- [14] W. NÖBAUER, *Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen*, Monatsh. Math., 59 (1955), pp. 194–202.
- [15] ———, *Polynomfunktionen auf primen Restklassen*, Arch. Math. (Basel), 39 (1982), pp. 431–435.
- [16] I. G. ROSENBERG, *Polynomial functions over finite rings*, Glas. Mat., 10 (1975), pp. 25–33.
- [17] Q. WEI AND Q. ZHANG, *On strong orthogonal systems and weak permutation polynomials over finite commutative rings*, Finite Fields Appl., 13 (2007), pp. 113–120.

- [18] Q. J. WEI AND Q. F. ZHANG, *On permutation polynomials in two variables over $\mathbb{Z}/p^2\mathbb{Z}$* , Acta Math. Sin. (Engl. Ser.), 25 (2009), pp. 1191–1200.
- [19] Q. ZHANG, *Polynomial functions and permutation polynomials over some finite commutative rings*, J. Number Theory, 105 (2004), pp. 192–202.

S. F.

Institut für Mathematik A
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
`frisch@tugraz.at`

D. K.

Institut für Mathematik B
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
`krenn@math.tugraz.at`